REMARKS

Claims 1-10 are rejected in the Office Action. Claims 1, 3-6, and 9-10 are amended, and no claims are cancelled. Accordingly, claims 1-10 remain pending.

REJECTIONS UNDER 35 USC §101

In "Claim Rejections – 35 USC §101" item 5 on page 3 of the above-identified Office Action, the Examiner rejects claims 1-10 as being directed to non-statutory subject matter. More specifically, the Examiner asserts that the operations of claim 1 do not produce a tangible result. According to the Examiner, the ultimate result of claim 1 is "producing a shared secret key." The Examiner then states that "producing" in its broadest sense is no more than "calculating", and is thus merely performing a mathematical operation. The key must be produced and stored, according to the Examiner, for the method to have a tangible result.

In response, while Applicant does not agree with the Examiner's reading, Applicant has amended claim 1 as the Examiner has suggested, reciting that the shared secret key is produced "in memory of the computing device." Accordingly, Applicant believes that claim 1 is patentable under §101.

Claims 2-10 depend from claim 1, and accordingly are patentable under §101 for at least the same reasons.

REJECTIONS UNDER 35 USC §103

In "Claim Rejections – 35 USC §103" item 6 on page 4 of the above-cited Office Action, the Examiner rejects claims 1-10 as being unpatentable over U.S. Patent No. 6,118,873 to *Lotspiech et al.* (hereinafter "Lotspiech") in view of U.S. Patent No. 5,412,729 to *Liu* (hereinafter "Liu") under 35 USC §103(a).

Amended claim 1 recites a "method comprising:

receiving, by a computing device, a key matrix having N rows and M columns of matrix keys, where N≥2 and M≥2;

for each column of the key matrix, performing, by the computing device, arithmetic operations utilizing matrix keys of at least two selected rows of the key matrix to produce a secret device key which is part of a first set of secret device keys;

producing, in memory of the computing device, by the computing device, a shared secret key based on arithmetic operations on selected secret device keys of the first set of secret device keys, the selected secret device keys being a portion of the first set of secret device keys and being determined based on a first key selection vector received from a recipient digital platform."

In contrast, Lotspiech merely teaches a method of encryption where session identifiers are combined with device keys to create an encoding matrix. In Lotspiech, each of a plurality of recipient devices is assigned "N device keys", N being equal to the number of columns in a matrix of device keys. While two or more device keys of the matrix may belong to the same row, no two may belong to the same column for any device. After assigning, randomly generated session numbers are applied to all device keys of the matrix, and the resulting encoding matrix is included with messages to recipients to encrypt those messages.

On pages 4-5 of the Office Action, the Examiner equates the matrix keys of claim 1 to the device keys, the secret device key to the set of device keys assigned a device, and the first set of secret device keys to the collective of the sets of device keys assigned the plurality of recipients.

Even assuming the Examiner's position for the sake of argument (Applicant does not agree with the Examiner's position, but this need not be addressed at this time), Lotspiech nonetheless fails to teach "producing, by the computing device, a shared secret key based on arithmetic operations on selected secret device keys of the first set of secret device keys, the selected secret device keys being a portion of the first set of secret device keys and being determined based on a first key selection vector received from a recipient digital platform," as is claimed by

amended claim 1. The only thing capable of reading on the "shared secret key" disclosed by Lotspiech is the encoding matrix illustrated by Figure 5 of Lotspiech. The encoding matrix of Lotspiech, however, is produced based on application of session identifiers to all device keys, not to selected device keys, which comprise only a portion of the secret device keys, determined based on a selection vector received from a recipient digital platform, as is required by amended claim 1.

Additionally, Liu does not cure this deficiency. Liu merely teaches a method of mapping between ciphertext and plain text vectors, including inverting rows and columns of a matrix of keys. It is for such row/column inversion that the Examiner cited Liu (in Lotspiech, the columns and rows have inverse roles from the columns and rows recited by claim 1). Like Lotspiech, however, Liu does not teach or suggest "producing, by the computing device, a shared secret key based on arithmetic operations on selected secret device keys of the first set of secret device keys, the selected secret device keys being a portion of the first set of secret device keys and being determined based on a first key selection vector received from a recipient digital platform" as recited by amended claim 1.

Accordingly, amended claim 1 is patentable over Lotspiech and Liu, alone or in combination, under §103.

Claims 2-10 depend from claim 1, incorporating its limitations. Thus, for at least the same reasons discussed above, claims 2-10 are patentable over Lotspiech and Liu, alone or in combination, under §103.

Conclusion

Applicants respectfully assert that claims 1-10 are in condition for allowance. Entry of the foregoing is respectfully requested and a Notice of Allowance is earnestly solicited. Please charge any shortages and credit any overages to Deposit Account No. 500393.

Respectfully submitted,
SCHWABE, WILLIAMSON & WYATT

Dated: May 9, 2007

/Robert C. Peck/
Robert C. Peck
Registration No. 56,826

Pacwest Center, Suites 1600-1900
1211 SW Fifth Avenue
Portland, Oregon 97204
Telephone: 503-222-9981